УДК 581.3

К.В. Горопаха, Ю.М. Кладій, А.М. Гринчук, В.Р. Слободян
Тернопільський національний економічний університет, Україна

АЛГОРИТМИ ПОШУКУ ОБЕРНЕНОГО ЕЛЕМЕНТА ЗА МОДУЛЕМ

K.V. Horopakha, Yu.M. Kladij, A.M. Hrynchuk, V.R. Slobodjan

THE ALGORITHMS OF FINDINGS OF INVERSE ELEMENT BY MODULE

Операція пошуку мультиплікативного оберненого елемента за модулем на даний час є однією з найважливіших і одночасно найбільш обчислювально складних в сучасній теорії чисел [1]. Мультиплікативно оберненим до числа a за модулем n називається таке число b, для якого виконується рівність $a \cdot b \bmod n = 1$, тобто $b = a^{-1} \bmod n$. Числа a та n при цьому повинні бути взаємно простими. В [2] описані методи пошуку оберненого елемента, з яких найбільш поширеними є такі: перебором всіх можливих варіантів; за допомогою теореми Ейлера; на основі розширеного алгоритму Евкліда.

Перший метод характеризується високою обчислювальною складністю, оскільки повний перебір вимагає значних часових затрат.

При використанні теореми Ейлера $a^{\varphi(n)} \bmod n = 1$ отримується $a^{\varphi(n)-1} \bmod n = a^{-1} \bmod n$. Це передбачає виконання модулярного експоненціювання [3-4], що може привести до переповнення розрядної сітки процесора [5] і ускладнює пошук оберненого елемента для багаторозрядних чисел.

Найбільш поширеним є метод пошуку мультиплікативного оберненого елемента за модулем на основі розширеного алгоритму Евкліда. Даний метод характеризується великою кількістю ділень з остачею, перемножень і підстановок, хоча він володіє найменшою часовою складністю в порівнянні з іншими двома, наведеними вище.

Метою даної роботи є розробка нових методів пошуку оберненого елемента за модулем без виконання обчислювально складних операцій множення та ділення з остачею.

З теорії чисел відомо [1], що вираз $a \cdot b \bmod n = 1$ можна переписати таким чином: $a \cdot b = k \cdot n + 1$, де k – деяке ціле число. Звідси слідує, що для пошуку оберненого елемента необхідно до модуля додати 1 і перевірити, чи ділиться націло отримане число на a. Якщо не ділиться, то далі до отриманого числа потрібно послідовно додавати модуль до тих пір, поки результатом ділення не буде ціле число. Математично це записується так:

$$n_0 = n + 1;\ \ b_0 = (n+1)/a;$$
$$n_1 = 2 \cdot n + 1;\ \ b_1 = (2 \cdot n + 1)/a;$$
$$\ldots.$$
$$n_i = (i+1) \cdot n + 1;\ \ b_i = ((i+1) \cdot n + 1)/a;\ b_i \in Z.$$

В таблиці 1 наведено приклад застосування алгоритму пошуку оберненого елемента на основі додавання модуля.

Таблиця 1. Пошук оберненого елемента $41^{-1} \bmod 157$ на основі додавання модуля

i	0	1	2	3	4	5
n_i	158	315	472	629	786	943
b_i	3,85…	7,68…	11,51…	15,34…	19,17…	23

Отже, $41^{-1}\text{mod } 157=23$. Результат отриманий без використання громіздких операцій ділення з остачею та множення.

Для зменшення чисел, які використовуються в даній процедурі, можна додавати не модуль, а залишок $n_{00}=n \bmod a$ до тих пір, поки залишок від ділення отриманого результату на число a не буде дорівнювати 0. Математичний запис даного алгоритму матиме такий вигляд:

$$b_{01} = (n_{00} + 1) \bmod a;$$
$$b_{11} = (b_{01} + n_{00}) \bmod a;$$
$$b_{21} = (b_{11} + n_{00}) \bmod a;$$
$$\ldots.$$
$$b_{i1} = (b_{i-1\ 1} + n_{00}) \bmod a = 0.$$

Обернений елемент шукається за формулою $b = a^{-1} \bmod n = (i+1)n/a$.

В таблиці 2 наведено приклад застосування алгоритму пошуку оберненого елемента на основі додавання залишку з врахуванням, що $n_{00}=157 \bmod 41=34$. Отже, $41^{-1}\text{mod } 157=(6\cdot157+1)/41=23$. Кількість ітерацій даного алгоритму така ж сама, як і в попередньому, однак майже усі операції виконуються над набагато меншими числами.

Таблиця 2. Пошук оберненого елемента $41^{-1}\text{mod } 157$ на основі додавання залишку

i	0	1	2	3	4	5
b_{i1}	35	28	21	14	7	0

На відміну від розширеного алгоритму Евкліда, дані методи дозволяють розпаралелити процес пошуку оберненого елемента на декілька потоків. Початок обчислень в кожному потоці для методів додавання модуля та залишку відповідно визначається так: $N_0 = \left(\left[\frac{(j-1)a}{z}\right]+1\right)n+1$; $N_1 = \left(\left(\left[\frac{(j-1)a}{z}\right]+1\right)n_{00}+1\right) \bmod a$, де j - номер потоку, z - кількість потоків. Максимальна кількість ітерацій в кожному потоці становитиме $a/z+1$.

Отже, запропоновані методи ефективно можна використовувати для пошуку оберненого елемента за модулем.

Література

1. Виноградов И.М. Основы теории чисел / И.М.Виноградов. – Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003. – 176 с.
2. Вербіцький О.В. Вступ до криптології / О.В. Вербіцький. – Львів: ВНТЛ, 1998. – 246 с.
3. Kozaczko D. Vector Module Exponential in the Remaining Classes System / D.Kozaczko, M.Kasianchuk, I.Yakymenko, S.Ivasiev // Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015). - Warsaw, Poland. - V.1, September – 2015. - P.161–163.
4. Касянчук М.М. Експериментальне дослідження програмної реалізації методів модулярного експоненціювання / М.М.Касянчук, І.З.Якименко, Т.М.Долинюк, Н.А.Рендзеняк // Інформатика та математичні методи в моделюванні. – 2015. – Т.5, №4. – С. 376–382.
5. Rajba T. Research of Time Characteristics of Search Methods of Inverse Element by the Module / T. Rajba, A. Klos-Witkowska, S. Ivasiev, I. Yakymenko, M. Kasianchuk // Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2017) – Bucharest, Romania. – V.1. – September, 2017. – P.82–85.